AMENDMENTS TO THE CLAIMS

1. (currently amended): A method of conducting a transaction by a purchaser over a communications network, comprising:

(a) assigning to said purchaser a first payment account number having a status which changes over time using an assigning computer;

(b) providing a second payment account number associated with said first payment account number to a purchaser computer using an issuer computer, said second payment account number being reusable by the purchaser for any purchase in which said first payment account number could be used ~~for as long as the first payment account number is usable by the purchaser~~, and not being a transaction number and having an encryption key assigned thereto wherein providing said second payment account number comprises:

(i) sending identification information from a purchaser computer to an issuer computer ;

(ii) verifying said identification information using an issuer computer,

(iii) after verifying said identification information, using an issuer computer to provide secure payment software comprising said second payment number to a purchaser computer;

(c) sending data from a purchaser computer using said secure payment software to a merchant computer comprising: at least one of said second payment account number and a digital certificate that includes said second payment account number, the cardholder's card expiration date, the merchant identification number, and at least one of a generated message authentication code (MAC) and a digital signature generated by the secure payment application;

~~(c)~~ (d) requesting authorization for payment of said transaction with said second payment account number and not said first payment account number using a merchant computer;

~~(d)~~ (e) identifying said purchaser's first payment account number in response to said authorization request using an acquirer computer or an issuer computer ~~processor~~

programmed to discriminate between said second payment account number and said first payment account number with at least one translation key that can be used to translate between the second payment account number and first payment account number; and

~~(e)~~ (f) using ~~said~~ an acquirer computer or an issuer computer programmed to discriminate between said second payment account number and said first payment account number, responding to said authorization request based upon said status of said first payment account number at the time of the transaction.

2. (original): The method of Claim 1, wherein said authorization request includes a cryptographic code based on said encryption key, and wherein said response to said authorization request is further based on said cryptographic code.

3. (original): The method of Claim 2, wherein said status is a function of the credit balance available for use by said purchaser, which credit balance changes over time as a result of the purchases made by the purchaser.

4. (currently amended): A method of conducting a transaction by a purchaser over a communications network, comprising:

(a) assigning to said purchaser a first payment account number having a status which changes over time ,using an assigning computer;

(b) providing ~~said~~ a purchaser computer with a secure payment application which includes a cryptographic key that is unique to said account number and a pseudo account number, said pseudo account number having the same length as and associated with said first payment account number, and said pseudo account number being reusable by the purchaser for any purchase in which said first payment account number could be used ~~for as long as the first payment account number is usable by the purchaser~~ wherein providing said secure payment application comprises:

(i) sending identification information from a purchaser computer to an issuer computer ;

(ii) verifying said identification information using an issuer computer,

(iii) after verifying said identification information, using an issuer computer to provide secure payment software comprising said second payment number to a purchaser computer;

(c) sending data from a purchaser computer using said secure payment software to a merchant computer comprising: at least one of said second payment account number and a digital certificate that includes said second payment account number, the cardholder's card expiration date, the merchant identification number, at least one of a generated message authentication code (MAC) and a digital signature generated by the secure payment application

~~(c)~~ (d) providing ~~said~~ a purchaser computer with merchant data based on the transaction;

~~(d)~~ (e) generating a message authentication code as a function of at least said merchant data and said cryptographic key using a computer programmed ~~with logic for generating~~ to generate authentication codes and for cryptographic processing;

~~(e)~~ (f) providing to ~~said~~ a merchant computer said pseudo account number and said message authentication code and not said first payment account number;

~~(f)~~ (g) verifying that said merchant data is the correct data for the transaction using a merchant computer;

~~(g)~~ (h) requesting an authorization for payment of said transaction using a merchant computer, said authorization request not including said first payment account number but including said pseudo account number and sent to an acquirer computer or an issuer computer;

~~(h)~~ (i) recognizing said pseudo account number and cryptographically processing said pseudo account number to produce said first payment account number using ~~said~~ an acquirer computer or an issuer computer; and

~~(i)~~ (j) using ~~said~~ an acquirer or an issuer computer, responding to said authorization request based on the status of said first payment account number, and passing said response back without transmission of said first payment account number.

5. (original): The method of Claim 4 wherein said pseudo account number is indicated to be different from said first payment account number by a special identifier within the pseudo account number.

6. (original): The method of Claim 4 wherein said pseudo account number is indicated to be such by data within a transaction record.

7. (original): The method of Claim 4 wherein said cryptographic key is a secret key.

8. (previously presented): The method of Claim 4 wherein said cryptographic key is a private key and said secure payment application further includes a card-unique certificate for the a corresponding public key and said message authentication code comprises a digital signature generated by said secure payment application.

9. (original): The method of Claim 4 wherein said pseudo account number is obtained by encrypting the associated first payment account number utilizing DESX methodology.

10. (original) The method of claim 4 wherein said pseudo account number is converted back into its associated first payment account number utilizing DEA with a double-length key.